



Cryptographic Centre of Excellence Services

Cryptographic Health Check

Professional Services

Schedule

Overview

Entrust's Cryptographic Center of Excellence ("CryptoCoE") portfolio of Professional Services provides the Customer with the consulting services and expertise needed for the Customer to build its own cryptographic center of excellence. Under this Cryptographic Health Check Offering, Entrust will interview key Customer personnel and analyze the Customer's governance and management of cryptography, leading to a report of findings, analysis and actionable recommendations to improve cryptographic health in the environment.

The Agreement for the Cryptographic Health Check Offering is made up of this Schedule, the Entrust General Terms and Conditions available at <https://www.entrust.com/general-terms.pdf> ("General Terms"), and an applicable Order. Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. Definitions.

- 1.1. "Cryptographic Governance" means the processes, policies and organizational structure that the Customer has established to manage its Cryptographic Estate.
- 1.2. "Cryptographic Estate" means the cryptographic algorithms, artifacts (e.g. keys and certificates), systems for managing cryptography, and devices for the secure management of cryptographic artifacts (e.g. hardware security modules) within a customer's IT systems.
- 1.3. "Cryptographic Health Check" means the professional services offered under the terms of this Schedule.
- 1.4. "Cryptographic Health Check Report" means the report described in Section 3.1.1.
- 1.5. "Cryptographic Policy Documentation" means the set of documented processes and procedures describing the governance of cryptography within an organization, which may include documentation specifying cryptographic policy generally, or policy documentation specific to solutions such as PKI (e.g. certificate policies and certification practice statement(s) as defined in RFC 3647).

2. Scope of Services.

- 2.1. Scope. Entrust will provide a consultant, who will review the Customer's current Cryptographic Governance and Cryptographic Estate via a sequence of remote meetings. Each remote meeting will be a single session not to exceed three (3) hours in duration. The scope of the review will cover a single set of Cryptographic Policy Documentation, consisting of up to five (5) individual policy related documents, if available, as well as an inventory of the Cryptographic Estate, if available. Gaps in policy coverage will be identified. The engagement is divided into four stages, which are detailed, along with the respective responsibilities of Entrust and Customer at each stage, in the table below. These steps will be completed for each engagement. The scope of Customer's Cryptographic Estate which can be covered by the Cryptographic Health Check Report will be determined by Entrust based on the workshops and documentation reviews described in this Section.

Stage 1: Kickoff
A single remote meeting

Entrust Responsibilities:

- Assign a project manager
- Contact Customer's project manager to schedule the project kickoff meeting, confirm attendee roles, and identify key participants.
- Schedule and facilitate the project kickoff meeting, where Entrust will explain the engagement process and provide an overview of best practices for management of a Cryptographic Estate
- Schedule the subsequent engagement steps and explain dependencies
- Identify required attendees for future sessions

Customer Responsibilities:

- Assign a project manager (or equivalent) to manage Customer resources listed below, as confirmed in kickoff planning discussions, and ensure their attendance at kickoff meeting:
 - Identify a representative of the policy authority for the organization who is responsible for defining and overseeing cryptographic policy (if applicable)
 - Engage stakeholders who can provide details of current Customer Cryptographic Estate, including systems for managing cryptography such as key management systems and Public Key Infrastructure(s)
- Gather information requested during the kick-off meeting and provide to Entrust

****Note:** *The scope of the Customer's Cryptographic Estate may vary depending on the size and/or complexity of Customer's environments. Therefore, the specific areas to be covered by the Cryptographic Health Check Report will be discussed during the planning meetings (i.e. meetings described in 'Stage 1' and 'Stage 2') and aligned with the limited number of workshops and documentation reviews included in the Offering. Entrust will determine the appropriate scope which can be included in the Cryptographic Estate to be reviewed. Should Customer require a more comprehensive health check of their Cryptographic Estate to address additional aspects of their environment, a separate professional services agreement will need to be established.*

Stage 2: Interview Workshops
Up to 4 remote meetings

Entrust Responsibilities:

- Facilitate the workshops and provide an agenda for each session in advance to allow Customer to ensure attendance of appropriate stakeholders and/or Customer's functional teams.
- Gather information about the current Customer processes, cryptographic policies, and the current Cryptographic Estate
- Entrust will attend each meeting making commercially reasonable efforts to review any materials previously provided by the Customer, if any, and provided such materials were supplied reasonably far in advance of the workshop.
- Review the Customer's operational and maintenance processes, as presented by Customer's stakeholders, to assess whether suitable steps are being taken to assure the long-term efficiency of the Cryptographic Estate in respect of security, reliability and recovery

Customer Responsibilities:

- Engage appropriate stakeholders for each workshop based on function and workshop agenda
- Provide Cryptographic Policy Documentation set for Entrust review if available
- Provide relevant cryptographic system architecture/design document (if available) or information on how business applications leverage the Cryptographic Estate
- Provide technical information/inventory of cryptographic assets deployed within the Cryptographic Estate (including algorithms, keys, libraries, digital certificates) if available

Stage 3: Report Preparation

Entrust Responsibilities:

- Analyze information submitted in Stage 2 meetings and reach out to Customer for any remaining or follow-up questions that arise during Stage 3 analysis.
- Produce the Cryptographic Health Check Report

Customer Responsibilities:

- Respond to Entrust questions if required in the case that Entrust required further detail or clarifications during report production.

**Stage 4: Report Presentation
Includes a single remote meeting**

Entrust Responsibilities:

- Provide Customer with initial Report.
- Meet with Customer to review the Cryptographic Health Check Report and discuss the recommendations.
- After this meeting, the report may be updated based on customer feedback to produce the final version of the report.

****Note:** There are no additional iterations of the report once the final version is delivered to Customer after the Report Presentation.

Customer Responsibilities:

- Ensure the appropriate Customer resources are available to attend the report presentation in order to provide feedback on the report.
- Provide feedback on the report to be incorporated into final version if applicable.

- 2.2. Project Managers. Entrust will assign a project manager (“PM”) who will have overall responsibility for ensuring delivery of the Cryptographic Health Check to the Customer. The PM is the Customer’s single point of contact with Entrust for the duration of the engagement, providing co-ordination of resources, tracking and closure of action items, and schedule, requirements and financial management.

Customer will assign a project manager to act as a single point of contact for Entrust, to ensure suitably qualified technical and business resources are available to fulfill the Customer’s responsibilities at the required times indicated in the table above.

- 2.3. Additional Work. If Customer requests work beyond the scope of this engagement, the Customer and Entrust may mutually agree to enter into a separate Professional Services Agreement to define the terms and scope of such additional services.

3. Deliverables.

- 3.1. Entrust will provide the following deliverable(s) (“Deliverables”) for each Cryptographic Health Check engagement:

- 3.1.1. A Cryptographic Health Check Report comprising:

- Executive summary
- Introduction and background
- Best practices and compliance recommendation
- Summary of current state of cryptographic policies and processes within Customer environment

- Highlight identified issues with root cause(s) and recommendation
 - Propose changes to policy documentation set and processes
- 3.2. Entrust delivers all documents to its customers in Adobe Acrobat PDF format. This eliminates dependence on a common word processor, provides document integrity and reduces the possibility of transmitting macro viruses to our customers. Upon request, Entrust can also deliver documents in Microsoft Word format.
- 3.3. Entrust is committed to delivering high quality services and products to its customers. All Deliverables will be subject to peer review and require Entrust Project Manager approval before being delivered to Customer. This also applies to situations where Entrust has chosen to sub-contract certain activities or Deliverables to our partner organizations.
4. **Dependencies and Assumptions.** Customer acknowledges and agrees that performance of the Cryptographic Health Check by Entrust will be subject to the dependencies and assumptions noted below.
- 4.1. All work to be performed during regular business hours.
- 4.2. All work to be performed remotely unless otherwise expressly agreed. In such a case, on-site work is billed on a time and materials basis. Entrust incurred travel and living expenses are billed at cost and paid by Customer. Travel time is billable to Customer at fifty percent (50%) of Entrust's then-current per diem rates.
- 4.3. Entrust reserves the right to fulfill delivery of the Cryptographic Health Check using Entrust employed staff, contractors or sub-contractors with appropriate experience and skills.
- 4.4. Any Entrust products provided to or used by Customer in relation to the engagement shall be subject to Entrust's standard terms and conditions for such products (unless otherwise agreed to between Entrust and Customer).
- 4.5. All third party products/components shall be supported by Entrust integrations as set out in the current Entrust product related documentation.
- 4.6. Entrust personnel shall not be made available or placed on stand-by for non-Entrust tasks or tasks unrelated to the Cryptographic Health Check.
5. **Customer Obligations.** Customer shall be responsible for the timely performance of its obligations under this Schedule, including the obligations below. Customer acknowledges that any delay on its part in the performance of its obligations may affect Entrust's provision of the Professional Services.
- 5.1. Provide Entrust with such information and materials as described in Section 2.1 or as Entrust may reasonably require to supply the Cryptographic Health Check and ensure that such information is complete and accurate in all material respects.
6. **Out of Scope.**

The following activities/tasks fall outside the scope of the Cryptographic Health Check. Entrust does offer customized Professional Services and may be able to assist the Customer with some of the tasks below in a separate engagement under a statement of work:

- Remediation work, including in particular remediation of any issues highlighted in the Cryptographic Health Check Report
- Provision of any content for policy, procedural or operational documentation.
- Formal project reporting (although informal status reporting will be provided).
- Installation and configuration of Entrust software
- Provision, installation or configuration of Entrust or third party hardware, software, operating systems or supporting network components.
- Development of custom code, including development or customization of any component or application.

- Development and/or execution of a formal test plan.
- Installation or configuration of a database or directory.
- Detailed build or customized documentation (i.e. operations guides).
- On-call/stand-by availability.
- Travel or any work on Customer's premises (except as specifically set out herein).
- All Professional Services not specifically identified in this Schedule.

7. **Scheduling.**

- 7.1. The actual start and completion dates of the Professional Services are dependent upon Entrust resource availability and Customer resource availability.
- 7.2. Cancellation/Rescheduling by Customer. Requests by Customer to cancel or reschedule a Professional Services engagement must be submitted in writing only via email to the assigned Entrust PM. Requests by phone or voicemail will not be accepted by Entrust. If Customer cancels or reschedules the Professional Services within five (5) business days of the scheduled engagement start date, Entrust reserves the right to charge a cancellation fee, equal to the value of one (1) day of Entrust consulting fees as set forth in Entrust' price list in effect at that time. Customer will reimburse Entrust for the costs incurred by Entrust due to Customer's cancellation or rescheduling. New engagements dates requests shall be established by mutual agreement only up to a maximum of two (2) rescheduling dates. Subsequent requests shall be subject a cancellation fee per request.
- 7.3. Cancellation/Rescheduling By Entrust. In the event of an engagement cancellation by Entrust, Entrust shall provide a prorated credit for the unperformed Professional Services to be applied towards alternative engagement dates.

8. **Acceptance and Changes.**

- 8.1. Acceptance. Any Deliverable specified in this Schedule as requiring Customer sign-off or acceptance shall be considered complete and accepted when it has been provided and reviewed by the Customer in accordance with the specified timelines, or if no timelines are specified, within ten (10) business days, and Customer has not provided Entrust with a written notice of rejection. Customer may only reject a Deliverable if it materially deviates from its specifications and the requirement in this Schedule. In the event of such a rejection Entrust shall correct the deviation and redeliver the Deliverable. After redelivery pursuant to the previous sentence, the parties shall again follow the acceptance procedures set forth in this Section 8.1 (Acceptance). This Section, in conjunction with Customer's right to terminate for material breach where applicable, sets forth Customer's only remedy and Entrust's only liability for failure of a Deliverable.
- 8.2. Changes. The Cryptographic Health Check represents a defined-scope package of Professional Services with a fixed price, and are therefore not subject to a change management process. In the event that Customer requires additional Professional Services beyond the scope of this Schedule, including if any of Entrust's work or Deliverables need to be revised or repeated due to Customer's failure or errors in performing its obligations, these additional Professional Services may be provided pursuant to a separate statement of work agreed by the Parties. In the absence of any agreement on a separate statement of work, Entrust shall have no obligation to provide additional or modified Professional Services or Deliverables.

9. **Fees.** Customer will pay Entrust the costs and fees for the Cryptographic Health Check as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

10. **Warranty.** Entrust warrants that the Professional Services it provides as described in this Schedule shall be performed in a professional manner in keeping with reasonable industry standards.

11. **Term and Termination.**



- 11.1. Term. The Cryptographic Health Check Offering is sold on a one-time engagement basis. The Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect until the work identified in Stages 1 through 4 in Section 2.1 above is complete.
- 11.2. Customer Default. If Entrust's performance of any of its obligations under this Schedule is prevented or delayed by any act or omission by the Customer or failure by the Customer to perform any relevant obligation ("Customer Default"):
 - 11.2.1. without limiting or affecting any other right or remedy available to it, Entrust shall have the right to suspend performance of the Professional Services until the Customer remedies the Customer Default, and to rely on the Customer Default to relieve it from the performance of any of its obligations in each case to the extent the Customer Default prevents or delays the Entrust's performance of any of its obligations;
 - 11.2.2. Entrust shall not be liable for any costs or losses sustained or incurred by the Customer to the extent such costs or losses arise from Customer's failure or delay to perform any of its obligations as set out herein; and,
 - 11.2.3. the Customer shall reimburse Entrust for any costs or losses sustained or incurred by Entrust to the extent these arise from the Customer Default.